Cisco ASA 5500 Series Unified Communications Deployments

Overview

Businesses of all sizes are migrating to IP telephony in order to take full advantage of unified communications. Cisco® Unified Communications products can help businesses streamline their operations, increase employee productivity, optimize business communications, and enhance customer care. Because protecting a unified-communications-based network from attacks is crucial to maintaining business continuity and integrity, Cisco has built security features into its Unified Communications products, and augments this security with the Cisco ASA 5500 Series.

The Cisco ASA 5500 Series is a family of multifunction security appliances for small businesses, branch offices, enterprises, and data center environments. These appliances deliver market-leading voice and video security services for unified communications, including robust firewall, full-featured IP Security (IPsec) and Secure Sockets Layer (SSL) VPN, intrusion prevention, and content security features. For unified communications deployments, these platforms can protect up to 30,000 phones and deliver application inspection for the broadest range of unified communications protocols, including Skinny Client Control Protocol (SCCP), Session Initiation Protocol (SIP), H.323, Media Gateway Control Protocol (MGCP), Computer Telephony Interface Quick Buffer Encoding (CTIQBE), and Real-Time Transport Protocol (RTP) and Real-Time Transport Control Protocol (RTCP).

Cisco ASA 5500 Series Unified Communications Features

Cisco ASA 5500 Series Adaptive Security Appliances are designed to secure real-time unified communications applications such as voice and video. The Cisco ASA 5500 Series can be used to protect all of the critical elements of a unified communications deployment (network infrastructure, call control platforms, IP endpoints, and unified communications applications). The Cisco ASA 5500 Series delivers several security features that complement the embedded security within the unified communications system, providing additional layers of protection. These include:

- Dynamic and granular access control to prevent unauthorized access to unified communications services
- Threat protection for the unified communications infrastructure
- Network security policy enforcement to create and administer effective unified communications policies for applications and users
- Service protection to help ensure maximum uptime for unified communications applications
- Voice and video encryption services that enable customers to maintain their security policies while encrypting signaling and media to prevent eavesdropping. Voice and video encryption services using SSL/IPsec VPN are also available for extending unified communications to remote users

All contents are Copyright © 1992–2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Access Control

Access control is a basic security function that allows only authorized access to resources and services within a system. In a unified communications context, this is often related to providing network-layer access control to the Cisco Unified Communications Manager and other application servers as a first line of defense against attack. Restricting access to the Cisco Unified Communications Manager servers significantly reduces the risk of an attacker probing the system for vulnerabilities or exploiting access through unauthorized network channels.

Cisco ASA 5500 Series Adaptive Security Appliances are voice- and video-aware and are able to inspect and apply policy to the protocols (SIP, SCCP, H.323, MGCP) used in modern unified communications. Legacy network access control mechanisms such as access control lists (ACLs) are unable to deal with these more complex protocols with the granularity and dynamism required by most organizations.

Unlike traditional data applications, unified communications protocols dynamically negotiate how to communicate by exchanging port information within the signaling control channel. Static access control mechanisms such as ACLs are unable to track which ports to open and must therefore apply weak access controls, limiting the ability to implement effective access policies.

Cisco ASA 5500 Series Adaptive Security Appliances can dynamically track exactly which authorized connections should be opened and close them as soon as the session has ended. This level of control, combined with other intelligent services such as voice-protocol-aware Network Address Translation (NAT), distinguishes the Cisco ASA 5500 Series appliances from legacy mechanisms that are not suited to the requirements of modern unified communications protocols.

Threat Prevention

The Cisco ASA 5500 Series protects Cisco Unified Communications applications from a range of common attacks that threaten the integrity and availability of the system. These include call eavesdropping, user impersonation, toll fraud, and denial of service (DoS). Many of these attacks (in particular, DoS) can be launched by sending malformed protocol packets to attack the unified communications call control systems and applications. The Cisco ASA 5500 Series performs protocol conformance and compliance checking on traffic destined to critical unified communications servers (for example, making sure that media flowing through the appliance is truly voice media [RTP], or preventing attackers from sending malicious voice signaling that could crash the call control systems). By helping to ensure that signaling and media comply with standard RFCs, the Cisco ASA 5500 Series provides an effective first line of defense for critical systems.

In addition to checking protocol conformance, the Cisco ASA family's multifunction security services can be extended to provide intrusion prevention services. The Cisco ASA 5500 Series AIP-SSM module applies hardware-based intrusion prevention system (IPS) features to inbound traffic to stop known attacks against unified communications call control and application servers. The combination of protocol conformance and intrusion prevention provides a robust network-layer defense against common unified communications threats.

Network Policy

Unified communications deployments are often subject to the security policy requirements established by the organization's security department. With the Cisco ASA 5500 Series' sophisticated unified communications security features, organizations are able to apply granular,

All contents are Copyright © 1992–2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

application-layer policies to the unified communications traffic to meet security compliance requirements. For example, businesses can permit or deny calls from specific callers or domains, or can apply specific blacklists or whitelists. Network policies can be extended to endpoints and applications; for example, allowing only calls from phones registered to the call control server or denying applications such as instant messaging over SIP.

Service Protection

Maximizing uptime is a critical security concern for most organizations. The Cisco ASA 5500 Series is a high-performance, highly available (Active-Active and Active-Standby) platform, and offers rate limiting services to prevent overloading or DoS attacks against the unified communications infrastructure.

Voice and Video Encryption Services

For compliance or security policy reasons, organizations can be required to provide confidentiality to voice and video traffic. End-to-end encryption often leaves network security appliances “blind” to media and signaling traffic, which can compromise access control and threat prevention security functions. This can result in a lack of interoperability between the firewall functions and the encrypted voice, leaving businesses unable to satisfy both of their key security requirements.

The Cisco ASA 5500 Series is unique in its support of an encryption proxy solution (Transport Layer Security [TLS] Proxy) for Cisco Unified Communications systems. As a truly integrated and trusted device within the Cisco Unified Communications Manager authentication domain; voice and video endpoints can trust the platform and securely authenticate and encrypt traffic. The Cisco ASA 5500 Series, as a proxy, is able to decrypt these connections, apply the required threat protection and access control, and help ensure confidentiality by re-encrypting the traffic onto the Cisco Unified Communications Manager servers. This integration provides organizations with the flexibility to deploy all of the required security countermeasures rather than to settle for an inadequate subset.

The Cisco ASA also supports flexible, secure connectivity using SSL or IPsec VPN services that enable secure, high-speed voice and data communications among multiple office locations or remote users. The Cisco ASA 5500 Series supports quality of service (QoS) features to enable reliable, business-quality delivery of latency-sensitive applications such as voice and video. The QoS policies can be applied on a per-user, per-group, per-tunnel, or per-flow basis so that the proper priority and bandwidth restrictions are applied to voice and video flows. In addition, pre-connection posture assessment and security checks help ensure that VPN users do not inadvertently bring attacks to the network.

Deployment Topologies

As shown in Figure 1, the Cisco ASA 5500 Series can be used across the network to protect the call control system, endpoints, applications, and the underlying infrastructure from attacks. These topologies include:

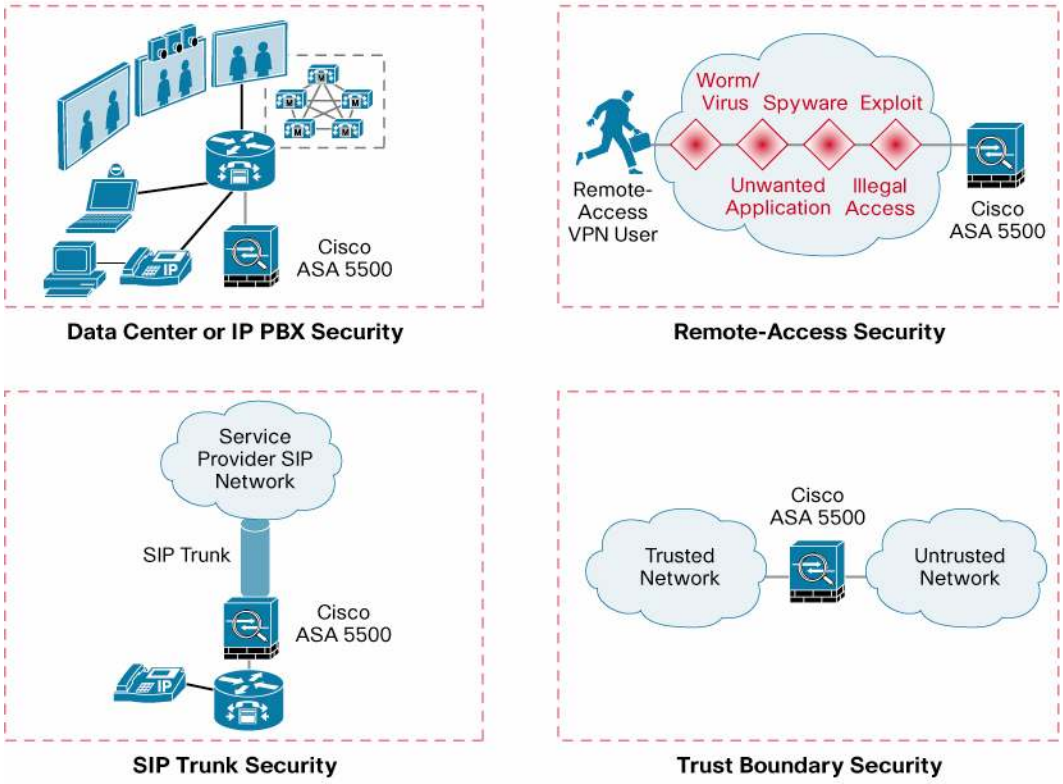
- **Protection of call control servers:** By controlling access from clients to these servers, the Cisco ASA 5500 Series can prevent malicious or unauthorized network connections from being made that could impact performance or availability. By statefully inspecting the connections to ascertain that they meet the access control policy and the connection conforms to expected behavior, the Cisco ASA platform provide a first line of defense for a secure unified communications deployment.

All contents are Copyright © 1992–2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- **Remote-access security:** The Cisco ASA 5500 Series delivers SSL and IPsec VPN services to provide secure connectivity for remote users (for example, teleworkers, mobile workers, and remote offices).
- **SIP trunk security:** Businesses are migrating to SIP trunk architectures to lower their communication costs. The Cisco ASA 5500 Series' robust SIP security capabilities provide protection from any attacks through SIP trunks.
- **Trusted/untrusted boundaries:** The Cisco ASA 5500 Series can also be positioned as a security device between a trusted and untrusted network to help ensure that vulnerabilities from the untrusted network do not impact the trusted network. This can include a Cisco ASA 5500 Series appliance being used to proxy traffic between voice and data VLANs, or a DMZ architecture where a Cisco ASA 5500 Series appliance is used to secure an internal network against external access.

With the range of Cisco ASA 5500 Series models available, organizations have the flexibility to standardize on a single family of security products while positioning specific models to meet different performance needs for every topology or location.

Figure 1. Cisco ASA 5500 Series Deployment Topologies



The Cisco ASA 5500 Series provides the most complete suite of voice and video security features for a unified communications network. Table 1 lists the features and benefits.

All contents are Copyright © 1992–2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Table 1. Features and Benefits Summary

Feature	Details
Unified Communications Application Inspection and Control	**SIP, SCCP, H.323, MGCP, RTP/RTCP, TCP, CTIQBE, RTSP**
SIP application inspection and control	• Enables deep inspection services for SIP traffic for both User Datagram Protocol (UDP) and TCP-based SIP environments. This provides granular control for protection against unified communications attacks. • Delivers protocol conformance support for numerous SIP RFCs, including RFC 3261. Delivers SIP state awareness and tracking and the ability to enforce mandatory header fields and absence of forbidden header fields, thus protecting businesses from attacks that use malformed packets. • Enables Network Address Translation and Port Address Translation (NAT and PAT)-based address translation support for SIP-based IP phones and applications such as Microsoft Windows Messenger, while delivering advanced services such as call forwarding, call transfers, and more. • Supports comprehensive threat defense features such as SIP state awareness and tracking, the ability to rate-limit SIP traffic to prevent DoS attacks, preventing SIP traffic from specific proxies to block SIP traffic from rogue proxy servers, and validation of RTP/RTCP for media. • Allows businesses to configure granular unified communications policies, such as permitting and denying callers and callees by configuring SIP Uniform Resource Identifier (URI) filters, inbound/outbound calls using whitelists and blacklists, permitting and denying use of applications such as instant messaging over SIP, or permitting and denying specific SIP methods (including user-defined methods).
H.323 security services	• Enables advanced H.323 inspection services that support versions 1–4 of the protocol along with Direct Call Signaling (DCS) and Gatekeeper Router Control Signaling (GKRCS) to provide flexible security integration in a variety of H.323-driven voice-over-IP (VoIP) environments. • Provides NAT and PAT support for H.323 services, including advanced features such as fax over IP (FoIP) using the T.38 protocol, an ITU standard that defines how to transmit FoIP in real time. • Supports threat prevention for H.323 traffic such as restricting call duration, preventing H.225 Registration, Admission, and Status (RAS) packets arriving out of state, and validation of RTP/RTCP for media. • Allows businesses to configure granular policies for H.323 services such as filtering on calling and called phone numbers to prevent rogue callers, and restricting services by filtering on specific media types.
SCCP security services	• Enables advanced SCCP inspection services for SCCP applications such as Cisco Unified IP Phones, Cisco Unified Personal Communicator, and Cisco IP Communicator to provide flexible security integration. • Supports comprehensive threat defense such as the ability to set the maximum SCCP message length to prevent buffer overflow attacks, the ability to tune timeouts for TCP SCCP connections and SCCP audio/video media connections, and validation of RTP/RTCP for media. • Allows businesses to configure granular policies for SCCP traffic such as enforcing only registered phone calls to send traffic through the Cisco ASA appliance and filtering on message IDs to allow or disallow specific messages.
MGCP security services	• Enables rich MGCP security services and NAT- and PAT-based address translation services for MGCP-based connections between media gateways and call agents or media gateway controllers.
Real-Time Streaming Protocol (RTSP) security services	• Enables inspection of RTSP protocols used to control communications between the client and server for streaming applications such as Cisco IP/TV®, Apple Quicktime, and RealNetworks RealPlayer. • RTSP security services deliver NAT- and PAT-based address translation services for RTSP media streams to improve support in real-time networking environments.
Fragmented and segmented multimedia stream inspection	• Enables inspection of H.323-, SIP-, and SCCP-based voice and multimedia streams that have been fragmented or segmented to prevent against these unique unified communications attacks.
Advanced TCP security engine	• Enables protection from several attacks, including protection for SYN flood attacks using SYNC cookies, protection for endpoints against protocol fuzzing, and retransmission-style TTL (time to live) evasion. • Delivers smart TCP proxy feature that reassembles TCP packets to protect against segment attacks that use multiple TCP packets. • Offers TCP traffic normalization services for additional techniques to detect attacks, including advanced flag and option checking, TCP packet checksum verification, detection of data tampering in retransmitted packets, and more.

All contents are Copyright © 1992–2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Feature	Details
RTP/RTCP inspection services	• Provides the ability to inspect RTP and RTCP traffic on media connections opened by the unified communications inspection engines, such as SIP and SCCP connections. • Allows businesses to set security policies for RTP/RTCP traffic such as validating conformance to RFC 1889, cross-checking media values between signaling and RTP to validate payload type, and policing of version number, payload type integrity, sequence numbers, and the synchronization source (SSRC).
Threat Prevention	**Threat Prevention**
Intrusion prevention services	• Optional Cisco ASA 5500 Series AIP-SSM Module applies intrusion prevention services to protect the unified communications infrastructure and call control servers from IPS signature-based attacks. The modules provide IPS services that have been optimized for unified communications and support specific unified communications engines such as the H.323/H.225 inspection engine, and help to prevent OS attacks on call control servers. • Unique intrusion prevention capabilities such as anomaly detection, OS fingerprinting capabilities, and risk rating features provide better context on threats to prevent against false positives.
Content security services	• Allows businesses to implement a gateway-based content inspection feature to inspect content of e-mail and Web traffic. This helps ensure that the unified communications infrastructure is free from viruses, worms, spam, phishing, and malware attacks.
Encryption Services	
TLS Proxy	• Addresses encrypted signaling and firewall integration issues where encrypted signaling leaves unified communications firewalls unable to dynamically open ports or apply policies. As a trusted device within the Cisco Unified Communications Manager system, the Cisco ASA appliance is able to intercept the encrypted signaling, mutually authenticate with the endpoint, and decrypt the signaling. Once the signaling is decrypted, the appliance is able to retrieve all the necessary signaling information and apply all the inspection and policy enforcement actions. To maintain secure connectivity from end to end, the appliance then initiates a secondary TLS session back to Cisco Unified Communications Manager. The signaling and communications between endpoint and Cisco Unified Communications Manager remain functionally the same and the firewall is able to deliver its unified communications security services • Supports TLS proxy services for both SIP and SCCP endpoints for comprehensive integration with Cisco Unified IP Phones.
SSL/IPsec VPN	• Delivers robust encrypted SSL and IPsec VPN services for both unified communications and data traffic, with preconnection posture assessment for endpoints and the ability to apply policies and inspection capabilities to VPN traffic to prevent remote users from bringing vulnerabilities to the network.

Ordering Information

To place an order, visit the Cisco Ordering Home Page. To download software, visit the Cisco Software Center.

There are two ways to order the Cisco ASA 5500 Series Adaptive Security Appliance. Organizations that are investing in a Cisco Unified Communications solution have the option to order a bundle that includes Cisco Unified Communications Manager and a Cisco ASA 5500 Series Adaptive Security Appliance. These bundles, when configured using the Dynamic Configurator tool or the Ordering Tool provide Cisco ASA 5500 Series model recommendations for every Cisco Unified Communications Manager server. For example:

- **Cisco MCS 7825 servers: Cisco ASA 5520** security appliances are recommended
- **Cisco MCS 7825 and 7835 servers: Cisco ASA 5540** security appliances are recommended
- **Cisco MCS 7825, 7835, 7845, and higher: Cisco ASA 5550** security appliances are recommended

Organizations that prefer to purchase their security appliances separately may purchase Cisco ASA 5500 Series bundles as described in Table 3. This table lists the more popular recommended options for Cisco Unified Communications deployments. The K8 unrestricted bundles (DES encryption only) are ideal for partners that do not have export licenses. An end customer can then

All contents are Copyright © 1992–2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

upgrade its platforms to support strong 3DES/AES encryption at http://www.cisco.com/go/license. This upgrade is available to customers at no cost.

Table 2. Secure Unified Communications Bundle Ordering Information

Product Name	Part Number
Cisco Secure Unified Communications Bundle (includes Cisco Unified Communications Manager 6.0)	SEC-Unified-CM-6.0 (available in Q1CY2008)
Cisco Secure Unified Communications Bundle (includes Cisco Unified Communications Manager 6.1)	SEC-Unified-CM.6.1 (available in Q1CY2008)

Table 3. Cisco ASA 5500 Series Ordering Information

Product Name	Part Number
Cisco ASA 5520 Adaptive Security Appliance with Integrated Firewall and VPN Services	
Cisco ASA 5520 Adaptive Security Appliance Firewall Edition; includes 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 750 IPsec VPN peers, 2 SSL VPN peers, Active/Active and Active/Standby high availability, Triple Data Encryption Standard/Advanced Encryption Standard (3DES/AES) license	ASA5520-BUN-K9
Cisco ASA 5520 Adaptive Security Appliance Firewall Edition; includes 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 750 IPsec VPN peers, 2 SSL VPN peers, Active/Active and Active/Standby high availability, DES license	ASA5520-K8
Cisco ASA 5520 Adaptive Security Appliance with Integrated Firewall, VPN, and IPS Services	
Cisco ASA 5520 Adaptive Security Appliance IPS Edition; includes Advanced Inspection and Prevention Security Services Module 20 (AIP-SSM-20), firewall services, 750 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 3DES/AES license	ASA5520-AIP20-K9
Cisco ASA 5520 Adaptive Security Appliance IPS Edition; includes AIP-SSM-20, firewall services, 750 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 3DES license	ASA5520-AIP20-K8
Cisco ASA 5540 Adaptive Security Appliance with Integrated Firewall and VPN Services	
Cisco ASA 5540 Adaptive Security Appliance Firewall Edition; includes 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 5000 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES license	ASA5540-BUN-K9
Cisco ASA 5540 Adaptive Security Appliance Firewall Edition includes 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 5000 IPsec VPN peers, 2 SSL VPN peers, DES license	ASA5540-K8
Cisco ASA 5540 Adaptive Security Appliance with Integrated Firewall, VPN, and IPS Services	
Cisco ASA 5540 Adaptive Security Appliance IPS Edition; includes AIP-SSM-20, firewall services, 5000 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 3DES/AES license	ASA5540-AIP20-K9
Cisco ASA 5540 Adaptive Security Appliance IPS Edition; includes AIP-SSM-20, firewall services, 5000 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 3DES license	ASA5540-AIP20-K8
Cisco ASA 5550 Adaptive Security Appliance with Integrated Firewall, and VPN Services	
Cisco ASA 5550 Adaptive Security Appliance Firewall Edition; includes 8 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 4 Gigabit Ethernet Small Form Factor Pluggable (SFP) interfaces, 5000 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES license	ASA5550-BUN-K9
Cisco ASA 5550 Adaptive Security Appliance Firewall Edition; includes 8 Gigabit Ethernet interfaces, 1 Fast Ethernet interface, 4 Gigabit Ethernet SFP interfaces, 5000 IPsec VPN peers, 2 SSL VPN peers, DES license	ASA5550-K8

Service and Support

Cisco Services make networks, applications, and the people who use them work better together.

Today, the network is a strategic platform in a world that demands better integration between people, information, and ideas. The network works better when services, together with products, create solutions aligned with business needs and opportunities.

All contents are Copyright © 1992–2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

The unique Cisco Lifecycle approach to services defines the requisite activities at each phase of the network lifecycle to help ensure service excellence. With a collaborative delivery methodology that joins the forces of Cisco, our skilled network of partners, and our customers, we achieve the best results.

For More Information

For more information about the Cisco ASA 5500 Series Adaptive Security Appliance, visit http://www.cisco.com/go/asa or contact your local account representative.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Printed in USA C78-450091-00 01/08

All contents are Copyright © 1992–2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.